

Practice questions RHCSA

- Don't forget to restore all VMs to the snapshots you have taken after lab configuration!

q1- Break into node2 and set the password as password. Set the target as multi-user and make sure it boots into that automatically. Reboot to confirm.

q2 - Configure the network interfaces and hostnames on both servers.

node1:

ip: 172.29.159.100

netmask: 255.255.255.0

gateway: 172.29.159.1

dns: 172.29.159.150

hostname: node1

node2:

ip: 172.29.159.200

netmask: 255.255.255.0

gateway: 172.29.159.1

dns: 172.29.159.150

hostname: node2

q3 - Enable ssh access for root on both servers. Connect with ssh key to root on both servers.

q4 - set yum repositories on both node1 and node2 to

BaseOS = <http://172.29.159.150/reposerver>

q5 - In node1, httpd service has some files in /var/www/html (do not change or alter files).

fix httpd service is not running on port 82.

Try to access it under <http://172.29.159.100:82>

q6 - Create the following users, groups, and group membership in node1:

- A group named sysadm.

- A user "harry" who belongs to sysadm as a secondary group.

- A user "natasha" who belongs to sysadm as a secondary group.

- A user "sarah" who does not have access to an interactive shell & who is not a member of sysadm group.

- "harry", "natasha", and "sarah" should all have the password of 'password'.

- "sysadm" group can add users.

- "harry" user has access to set password for users without prompting sudo password.

q7 - on node1 create a collaborative directory /shared/sysadm with the following characteristics:

Group ownership of /shared/sysadm is sysadm.

The directory should be readable, writable, and accessible to members of sysadm, but not to any other users.

Files created in /shared/sysadm automatically have group ownership set to the sysadm group.

q8 - on node1 Set The Cron Job for the user Natasha that runs at monday every 2 minutes from 15:00 to 16:00 local time and executes "Ex200 Testing" with logger.

q9 - on node1 Configure autofs to automatically mount moshe's (uid 2000) home directories from /export/home on 172.29.159.150 to /mnt/autofs_home/moshe

q10 - Configure both servers to create files with 660 permissions by default.

q11 - Set password policies to require a minimum of 8 characters and a maximum age of 60 days on one of the nodes.

q12 - Write a script named awesome.sh under /root on node 1:

- a) If “me” is given as an argument, then the script should output “Yes, I’m awesome.”
- b) If “them” is given as an argument, then the script should output “Okay, they are awesome.”
- c) If the argument is empty or anything else is given, the script should output “Usage
./awesome.sh me|them”

q13 - Configure NTP synchronization on both servers. Point them to 172.29.159.150.

q14 - On node2, create a new 2GiB volume group on /dev/vda named "platforms_vg"

q15 - Under the "platforms_vg" volume group, create a 500MiB logical volume name "platforms_lv" and format it as ext4.

q16 - Mount it persistently under /mnt/platforms_lv.

q17 - Extend the "platforms_lv" volume and partition by 500MiB.

q18 - On node2, create a 500MiB swap partition on /dev/vda and mount it persistently.

q19 - On node2, using the remaining space on /dev/vda, create a volume group with the name networks_vg.

q20 - Under the "networks_vg" volume group, create a logical volume with the name networks_lv. Ensure it uses 8 MiB extents. Configure the volume to use 75 extents. Format it with the vfat file system and ensure it mounts persistently on /mnt/networks_lv.

q21 - On reposerver, as the user cindy, create a container image from <http://172.29.159.150/Containerfile> with the tag web_image.

q22 - From the newly created image, deploy a container as a service with the container name cindy_web. The web config files should map to ~/web_files, and the local port of 8000 should be

mapped to the container's port 80. Create a default page that says "Welcome to Cindy's Web Server!". The service should be enabled and the website should be accessible. (Need full internet access for this question since we didn't configure a container registry. So do this question after configuring internet access or do it on the reposerver)

Important!!

umask might mess up with this question. resolve back umask to the default value before doing this question.

EXTRA QUESTIONS:

Q1 - Configure /var/tmp/fstab permissions

Copy the file /etc/fstab to /var/tmp/fstab . Configure the permissions of /var/tmp/fstab to meet the following conditions:

File /var/tmp/fstab owned by root user

File /var/tmp/fstab belongs to group root

The file /var/tmp/fstab should not be executable by anyone.

User natasha can read and write to /var/tmp/fstab.

User harry cannot write or read /var/tmp/fstab.

All other users (current or future) can read /var/tmp/fstab.

Q2 - Find all files owned by sshd and place a copy of them in the /root/findfiles directory.